

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A wireless ad-hoc communication system including a plurality of terminals, the communication system comprising:

a first terminal configured to encrypt a payload of a broadcast frame and to transmit the broadcast frame; and

a second terminal configured to receive the broadcast frame and to decode the payload of the broadcast frame, wherein

the first terminal is configured to encrypt the payload of the broadcast frame using a broadcast encryption key assigned to the first terminal, [[and]]

the second terminal is configured to decode the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal, and

any terminal in the plurality of terminals may perform the role of said first terminal or said second terminal.

Claim 2 (Previously Presented): The wireless ad-hoc communication system according to claim 1, wherein the second terminal includes:

an encryption-key management list table having at least an encryption-key management list including a set of a terminal identifier of the first terminal and the broadcast encryption key assigned to the first terminal;

means for searching the encryption-key management list table based on the terminal identifier of the first terminal included in an origination-terminal identifier of the received

broadcast frame to extract the corresponding broadcast encryption key assigned to the first terminal; and

means for decoding the payload of the broadcast frame using the extracted broadcast encryption key assigned to the first terminal.

Claim 3 (Previously Presented): The wireless ad-hoc communication system according to claim 1, wherein the first terminal includes:

a generated-key table configured to store the broadcast encryption key assigned to the first terminal;

means for encrypting the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal stored in the generated-key table; and

means for transmitting the encrypted broadcast frame.

Claim 4 (Previously Presented): A terminal comprising:

an encryption-key management list table having at least one encryption-key management list comprising a set of a terminal identifier of a different terminal and a broadcast encryption key assigned to the different terminal;

means for searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key; and

means for decoding a payload of the broadcast frame using the extracted broadcast encryption key.

Claim 5 (Previously Presented): A terminal comprising:

an encryption-key management list table having at least one encryption-key management list configured to store a unicast encryption key between said terminal and a different terminal and a broadcast encryption key assigned to the different terminal in association with a terminal identifier of the different terminal;

means for searching, when a destination-terminal identifier of a received frame is a broadcast address, the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of the frame to extract the corresponding broadcast encryption key as an encryption key, and when the destination-terminal identifier of the received frame is other than a broadcast address, searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of the frame to extract the corresponding unicast encryption key as the encryption key; and

means for decoding a payload of the frame using the extracted encryption key.

Claim 6 (Previously Presented): A terminal comprising:

a generated-key table configured to store a broadcast encryption key assigned to said terminal;

means for encrypting a payload of a broadcast frame using the broadcast encryption key; and

means for transmitting the encrypted broadcast frame.

Claim 7 (Previously Presented): A terminal comprising:

a generated-key table configured to store a broadcast encryption key assigned to said terminal;

an encryption-key management list table having at least one encryption-key management list configured to store a unicast encryption key between said terminal and a different terminal in association with a terminal identifier of the different terminal;

means for, when a frame to be transmitted is a broadcast frame, encrypting a payload of the broadcast frame using the broadcast encryption key of the generated-key table, and when the frame to be transmitted is a unicast frame, searching the encryption-key management list table for the encryption-key management list including a destination-terminal identifier of the unicast frame to encrypt a payload of the unicast frame using the corresponding unicast encryption key; and

means for transmitting the encrypted frame.

Claim 8 (Previously Presented): A terminal comprising:

means for encrypting a terminal identifier and a broadcast encryption key of the terminal using a unicast encryption key assigned to a transmission-destination terminal; and

means for transmitting the encrypted terminal identifier and broadcast encryption key of the terminal to the transmission-destination terminal.

Claim 9 (Previously Presented): A terminal comprising:

an encryption-key management list table having at least one encryption-key management list configured to store a broadcast encryption key of a different terminal in association with a terminal identifier of the different terminal;

means for encrypting the encryption-key management list using a unicast encryption key assigned to a transmission-destination terminal; and

means for transmitting the encrypted encryption-key management list to the transmission-destination terminal.

Claim 10 (Previously Presented): A terminal comprising:

means for receiving a terminal identifier and a broadcast encryption key of a different terminal from the different terminal;

means for encrypting the terminal identifier and the broadcast encryption key of the different terminal using a broadcast encryption key assigned to the terminal; and

means for broadcasting the encrypted terminal identifier and broadcast encryption key of the different terminal.

Claim 11 (Previously Presented): A method for decoding a broadcast frame in a terminal that includes an encryption-key management list table having at least one encryption-key management list including a set of a terminal identifier of a different terminal and a broadcast encryption key assigned to the different terminal, the method comprising:

searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key; and

decoding a payload of the broadcast frame using the extracted broadcast encryption key.

Claim 12 (Previously Presented): A method for encrypting a broadcast frame in a terminal that includes a generated-key table storing a broadcast encryption key assigned to said terminal, the method comprising:

encrypting a payload of the broadcast frame using the broadcast encryption key assigned to said terminal stored in the generated-key table; and

transmitting the encrypted broadcast frame.

Claim 13 (Previously Presented): A method for distributing a broadcast encryption key in a second terminal, the method comprising:

receiving a terminal identifier and a broadcast encryption key assigned to a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key assigned to the first terminal using the unicast encryption key;

encrypting a terminal identifier and a broadcast encryption key assigned to the second terminal using the unicast encryption key; and

transmitting the encrypted terminal identifier and broadcast encryption key assigned to the second terminal to the first terminal.

Claim 14 (Previously Presented): A method for distributing a broadcast encryption key in a second terminal, the method comprising:

receiving a terminal identifier and a broadcast encryption key assigned to a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key assigned to the first terminal using the unicast encryption key;

encrypting the terminal identifier and the broadcast encryption key assigned to the first terminal using a broadcast encryption key assigned to the second terminal; and

transmitting the encrypted terminal identifier and broadcast encryption key assigned to the first terminal to a third terminal.

Claim 15 (Previously Presented): A computer readable storage medium in which a program is recorded that causes a terminal including an encryption-key management list table having at least one encryption-key management list including a set of a terminal identifier of a transmission terminal and a broadcast encryption key assigned to the transmission terminal to execute a method comprising:

searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key; and

decoding a payload of the broadcast frame using the extracted broadcast encryption key.

Claim 16 (Previously Presented): A computer readable storage medium in which a program is recorded that causes a terminal including a generated-key table that stores a broadcast encryption key assigned to said terminal to execute a method comprising:

encrypting a payload of a broadcast frame using the broadcast encryption key stored in the generated-key table; and

transmitting the encrypted broadcast frame.



Claim 17 (Previously Presented): A computer readable storage medium in which a program is recorded that causes a second terminal to execute a method comprising:

receiving a terminal identifier and a broadcast encryption key of a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key of the first terminal using the unicast encryption key;

encrypting a terminal identifier and a broadcast encryption key of the second terminal using the unicast encryption key; and

transmitting the encrypted terminal identifier and broadcast encryption key of the second terminal to the first terminal.

Claim 18 (Previously Presented): A computer readable storage medium in which a program is recorded that causes a second terminal to execute a method comprising:

receiving a terminal identifier and a broadcast encryption key assigned to a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal;

decoding the encrypted terminal identifier and broadcast encryption key assigned to the first terminal using the unicast encryption key;

encrypting the terminal identifier and the broadcast encryption key assigned to the first terminal using a broadcast encryption key assigned to the second terminal; and

transmitting the encrypted terminal identifier and broadcast encryption key assigned to the first terminal to a third terminal.